

Chebotarëv Density and the Bateman-Horn constant

Timothy Foo

Abstract

This is an expository article on relating the Chebotarëv Density Theorem to the Bateman-Horn constant.

Mathematics Subject Classification (2010): 11C08, 11N05, 11N32

Keywords: Bateman-Horn conjecture, Bateman-Horn constant, Hardy-Littlewood conjecture F, Schinzel Hypothesis H, Chebotarëv Density Theorem, Merten's Third Theorem, orbit counting

Introduction

The following article is expository and discusses the Bateman-Horn constant. Let $f(x) \in \mathbb{Z}[x]$. According to the Bateman-Horn conjecture [B2], [BH], we should expect that

$$\sum_{n \leq x} \Lambda(f(n)) \sim C(f)x \quad (1)$$

where $\Lambda(n)$ is the Von Mangoldt function and $C(f)$ is called the Bateman-Horn constant and depends only on the polynomial f . Indeed, Hardy and Littlewood already made such conjectures for quadratic polynomials in the form of the Hardy-Littlewood Conjecture F [HL]. Furthermore, more precise heuristic arguments for primes in random sets can be found in [B], which we rely on here. Although the Bateman-Horn conjecture remains open, on average results for families of quadratic polynomials have been obtained in [BZ], [BZ2].

The Bateman-Horn constant is defined to be

$$C(f) = \prod_p \left(\frac{p - n_p}{p - 1} \right) \quad (2)$$

where n_p is the number of solutions to the equation $f(n) \equiv 0 \pmod{p}$ in $\mathbb{Z}/p\mathbb{Z}$.

Observe that the quantity n_p can only assume finitely many values, and in fact, for primes p not dividing $\Delta(f)$, the discriminant of f , the values it assumes are dependent only on the conjugacy class of the Frobenius element σ_p of p in the Galois group G of the splitting field of f , over \mathbb{Q} . This is a consequence of the theorems of Frobenius and Chebotarëv, which are the subject of very nice exposition in [LS]. More specifically, denote the degree of f by n , and for primes p not dividing $\Delta(f)$, let λ be a partition of n

corresponding to a certain *decomposition type* of $f \bmod p$. Then n_p is the number of 1s appearing in λ . Furthermore, the above *decomposition type* corresponds to the *cycle pattern* of the Frobenius element σ_p in G . For a conjugacy class \mathfrak{C} of G , all primes p having $\sigma_p \in \mathfrak{C}$ have the same value of n_p , so we can denote such n_p by $n_{\mathfrak{C}}$. For more information on n_p , which is interesting in its own right, we refer the reader to [D],[S].

Therefore, if we temporarily ignore considerations of convergence, we can write the Bateman-Horn constant as

$$C(f) = \prod_{p|\Delta(f)} \left(\frac{p - n_p}{p - 1} \right) \times \prod_{\mathfrak{C} \subset G} \prod_{\substack{p \\ \sigma_p \in \mathfrak{C}}} \left(\frac{p - n_{\mathfrak{C}}}{p - 1} \right). \quad (3)$$

But the theorems of Frobenius and Chebotarëv have an asymptotic flavour. Therefore, to apply them, we can rewrite the above as

$$C(f) = \prod_{p|\Delta(f)} \left(\frac{p - n_p}{p - 1} \right) \times \lim_{x \rightarrow \infty} \prod_{\mathfrak{C} \subset G} \prod_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C}}} \left(\frac{p - n_{\mathfrak{C}}}{p - 1} \right). \quad (4)$$

Theorems

As mentioned later, Merten's Third Theorem, Lemma 4 here, has been generalized to some specific arithmetic progressions in [U] and to general arithmetic progressions in [G],[LZ],[V], and [W]. (See Lemma 6 here.) It is not unreasonable to assume that it can further be generalized to conjugacy classes in Galois groups. While the above references might deal with error terms, we need here only a simple asymptotic formula for the main term. To do this, it is instructive to see section 6 of [LZ] where a simplified formula is given for the constant in front of the main term. By mimicking this for the case of conjugacy classes in Galois groups and then applying the Chebotarëv Density Theorem, we can prove Theorem 1 here.

Noting that, for $f \in \mathbb{Z}[x]$, the Bouniakowsky condition is the condition that

$$\gcd(\{f(n) : n \in \mathbb{Z}\}) = 1,$$

we have:

Theorem 1. *Let $f \in \mathbb{Z}[x]$ be irreducible and satisfying the Bouniakowsky condition. Let G be the Galois group of f and let \mathfrak{C} be a conjugacy class of G . Then there exists a constant $c_{\mathfrak{C},G} \neq 0$ such that*

$$\prod_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C} \subset G}} \left(1 - \frac{1}{p} \right) \sim c_{\mathfrak{C},G} (\log x)^{-|\mathfrak{C}|/|G|}$$

as $x \rightarrow \infty$.

Proof It will be instructive to see section 6 of [LZ], which asserts and proves, for $(l, k) = 1$, as $x \rightarrow \infty$, the asymptotic formula

$$\prod_{\substack{p \leq x \\ p \equiv l \pmod k}} \left(1 - \frac{1}{p}\right) \sim c_{l,k} (\log x)^{-1/\varphi(k)},$$

where the constant is given by

$$c_{l,k} = \left(e^{-\gamma} \prod_p \left(1 - \frac{1}{p}\right)^{\alpha(p;k,l)} \right)^{1/\varphi(k)},$$

with γ being the Euler-Mascheroni constant and

$$\alpha(p; k, l) = \begin{cases} \varphi(k) - 1, & \text{if } p \equiv l \pmod k \\ -1, & \text{otherwise.} \end{cases}$$

With this as a guide, we assert that the constant in the case of conjugacy classes for Galois groups is

$$c_{\mathfrak{C}, G} = \left(e^{-\gamma} \prod_p \left(1 - \frac{1}{p}\right)^{\alpha(p; G, \mathfrak{C})} \right)^{|\mathfrak{C}|/|G|},$$

with

$$\alpha(p; G, \mathfrak{C}) = \begin{cases} \frac{|G|}{|\mathfrak{C}|} - 1, & \text{if } \sigma_p \in \mathfrak{C} \subset G \\ -1, & \text{otherwise.} \end{cases}$$

We give a different proof from what occurs in [LZ]. By Merten's Third Theorem, Lemma 4, we have that as $x \rightarrow \infty$,

$$\begin{aligned} \prod_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C} \subset G}} \left(1 - \frac{1}{p}\right) &\sim \prod_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C} \subset G}} \left(1 - \frac{1}{p}\right) \times \left(\frac{\prod_{p \leq x} p/(p-1)}{e^\gamma \log x} \right)^{|\mathfrak{C}|/|G|} \\ &\sim \prod_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C} \subset G}} \left(1 - \frac{1}{p}\right) \times \left(\frac{\prod_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C} \subset G}} \left(1 - \frac{1}{p}\right)^{-1} \prod_{\substack{p \leq x \\ \sigma_p \notin \mathfrak{C} \subset G}} \left(1 - \frac{1}{p}\right)^{-1}}{e^\gamma \log x} \right)^{|\mathfrak{C}|/|G|} \\ &\sim \prod_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C} \subset G}} \left(1 - \frac{1}{p}\right)^{1 - \frac{|\mathfrak{C}|}{|G|}} \times \prod_{\substack{p \leq x \\ \sigma_p \notin \mathfrak{C} \subset G}} \left(1 - \frac{1}{p}\right)^{-\frac{|\mathfrak{C}|}{|G|}} \times \left(\frac{1}{e^\gamma \log x} \right)^{\frac{|\mathfrak{C}|}{|G|}} \\ &\sim \left(e^{-\gamma} \prod_p \left(1 - \frac{1}{p}\right)^{\alpha(p; G, \mathfrak{C})} \right)^{|\mathfrak{C}|/|G|} (\log x)^{-|\mathfrak{C}|/|G|} \end{aligned}$$

where the product over primes in the last line converges due to the Chebotarëv Density Theorem.

We will now state Theorem 2 of this article. It might seem odd to prove something which is evident already, but this article is only meant to serve an expository function by discussing the Bateman-Horn constant from this angle.

Theorem 2. *Let $f \in \mathbb{Z}[x]$. Then the Bateman-Horn constant $C(f)$ converges to a non-zero number if and only if f is irreducible and satisfies the Bouniakowsky condition.*

Examples and heuristics

The question of whether $C(f)$ converges to zero or not can be seen as a “competition” between the primes for which $n_{\mathfrak{C}} = 0$ and those for which $n_{\mathfrak{C}} > 1$. We also have the additional information that $C(f)$ ought to be 0 for reducible polynomials and nonzero for irreducible polynomials satisfying the Bouniakowsky condition. The motivation here is to understand how to differentiate between, for example, reducible and irreducible polynomials f . Thus for example, if the polynomial f is reducible, there should be too few primes having $n_{\mathfrak{C}} = 0$ to stop the Bateman-Horn constant from converging to 0. Let us try a few examples:

Example 1: $f(x) = x^3 + 2$

In this case, the map $x \rightarrow x^3$ is a bijection on $\mathbb{Z}/p\mathbb{Z}$ for primes $p \equiv 2 \pmod{3}$, so for such primes, we have $n_{\mathfrak{C}} = 1$ and they do not contribute to the product. On the other hand, for primes $p \equiv 1 \pmod{3}$, we have, by Chebotarëv’s Density Theorem, that $1/3$ of them will have $n_{\mathfrak{C}} = 3$ and $2/3$ of them will have $n_{\mathfrak{C}} = 0$. We observe that the primes for which $n_{\mathfrak{C}} = 3, 1, 0$ are in the ratio $1 : 3 : 2$ respectively. We now perform the following algorithm: Take the formal term

$$\frac{p - n_{\mathfrak{C}}}{p - 1}$$

and raise it to the power of the number occuring in the ratio corresponding to it. Then take the product over all \mathfrak{C} . For example, here we have

$$\left(\frac{p-3}{p-1}\right) \left(\frac{p-1}{p-1}\right)^3 \left(\frac{p}{p-1}\right)^2.$$

We observe that after expanding the numerators and denominators, so that we have polynomials of the same degree in the numerator and denominator, the coefficients of the term of second highest degree (the term $x^{|G|-1}$) are the same in both the numerator and denominator. We shall call this **Condition 1** and state the following lemma:

Lemma 0. *Condition 1 holds for all irreducible $f \in \mathbb{Z}[x]$ satisfying the Bouniakowsky condition.*

Proof See Theorem 5 of [B].

Example 2: $f(x) = x^7 - 7x + 3$

This example is taken from [V2]. Here we have $|G| = 168$ and we have *decomposition types* $(7), (4, 2, 1), (3, 3, 1), (2, 2, 1, 1, 1), (1, 1, 1, 1, 1, 1, 1)$ in the ratio $48 : 42 : 56 : 21 : 1$ respectively, corresponding to $n_{\mathfrak{C}} = 0, 1, 1, 3, 7$ respectively. The formal product

$$\left(\frac{p}{p-1}\right)^{48} \left(\frac{p-1}{p-1}\right)^{42} \left(\frac{p-1}{p-1}\right)^{56} \left(\frac{p-3}{p-1}\right)^{21} \left(\frac{p-7}{p-1}\right)$$

also satisfies **Condition 1**.

In fact, **Condition 1** is equivalent to the following condition which we shall call **Condition 1'**:

Condition 1'.

$$\sum_{\mathfrak{C} \subset G} n_{\mathfrak{C}} |\mathfrak{C}| = \sum_{\mathfrak{C} \subset G} |\mathfrak{C}| = |G|.$$

This says that when the polynomial f is factored over a random prime $p \nmid \Delta(f)$, then the expected number of solutions in $\mathbb{Z}/p\mathbb{Z}$ is 1. It is quite clear that **Condition 1'** is satisfied when G is abelian. For example, if f is the cyclotomic polynomial having $G = (\mathbb{Z}/m\mathbb{Z})^*$ for some m , then the conjugacy class \mathfrak{C} for which the polynomial f has *decomposition type* $(1, 1, \dots, 1)$ is simply $m\mathbb{Z} + 1$ and this has $n_{\mathfrak{C}} = \varphi(m)$. All other conjugacy classes yield $n_{\mathfrak{C}} = 0$. Each conjugacy class is just a single element of G . Therefore,

$$\sum_{\mathfrak{C} \subset G} n_{\mathfrak{C}} |\mathfrak{C}| = \varphi(m) \cdot 1 + 0 \cdot (\varphi(m) - 1) = \varphi(m) = |G|.$$

The point of **Condition 1** is to approximate

$$\prod_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C}}} \left(\frac{p - n_{\mathfrak{C}}}{p - 1} \right)$$

with

$$\prod_{p \leq x} \left(\frac{p - n_{\mathfrak{C}}}{p - 1} \right)^{\frac{|\mathfrak{C}|}{|G|}}.$$

We will then have that

$$C(f) \approx \prod_{p \mid \Delta(f)} \left(\frac{p - n_p}{p - 1} \right) \times \lim_{x \rightarrow \infty} \left(\prod_{p \leq x} \prod_{\mathfrak{C} \subset G} \left(\frac{p - n_{\mathfrak{C}}}{p - 1} \right)^{|\mathfrak{C}|} \right)^{\frac{1}{|G|}} \quad (5)$$

and **Condition 1** will ensure, by Lemma 1, the convergence to a nonzero number of the product

$$\prod_p \prod_{\mathfrak{C} \subset G} \left(\frac{p - n_{\mathfrak{C}}}{p - 1} \right)^{|\mathfrak{C}|},$$

thus also ensuring the converge to a nonzero number of $C(f)$. Likewise, for a reducible polynomial f , we expect that $C(f) = 0$. (5) ought to hold in

some form for reducible f , where this time we do not consider Galois groups or conjugacy classes but simply take the product over *decomposition types*. An analogue of **Condition 1** should fail for reducible f , thus allowing $C(f)$ to converge to 0. Lemma 2 will make this explicit. Also, in a subsequent section, we will try to make explicit the \approx in (5). We call this **Condition 2**.

Example 3: $f(x) = (x^2 + 1)(x^2 + 2)$

In this example, the polynomial f is reducible, and thus $C(f)$ should be 0. If we check **Condition 1**, we see that it fails. We have the *decomposition types* $(1, 1, 1, 1)$, $(1, 1, 2)$, $(2, 1, 1)$, $(2, 2)$ occurring in ratio $1 : 1 : 1 : 1$, respectively, giving $n_\lambda = 4, 2, 2, 0$ respectively, according to whether $\left(\frac{1}{p}\right) = \left(\frac{2}{p}\right) = 1$, $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = -1$, $\left(\frac{1}{p}\right) = -1$ and $\left(\frac{2}{p}\right) = 1$, or $\left(\frac{1}{p}\right) = \left(\frac{2}{p}\right) = -1$ respectively. Considering the formal term

$$\left(\frac{p-4}{p-1}\right) \left(\frac{p-2}{p-1}\right) \left(\frac{p-2}{p-1}\right) \left(\frac{p}{p-1}\right),$$

we see that the coefficient of the x^3 term is smaller in the numerator than in the denominator.

Definitions and Lemmas

We make the following definitions:

Given an integer r , we define the terms $E(\mathfrak{C}, G, r; x)$ and $E(r; x)$ as follows:

$$\sum_{\substack{p \leq x \\ p \nmid \Delta(f)}} \log(p - r) = x + E(r; x), \quad (6)$$

$$\sum_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C} \subset G}} \log(p - r) = \frac{|\mathfrak{C}|}{|G|} x + E(\mathfrak{C}, G, r; x). \quad (7)$$

Given integers $r_1 \neq r_2$, define $Q(\mathfrak{C}, G, r_1, r_2; x)$ by:

$$Q(\mathfrak{C}, G, r_1, r_2; x) = \left(\prod_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C}}} \frac{p - r_1}{p - r_2} \right) / \left(\prod_{\substack{p \leq x \\ p \nmid \Delta(f)}} \frac{p - r_1}{p - r_2} \right)^{\frac{|\mathfrak{C}|}{|G|}}. \quad (8)$$

Lemma 1. *Let $f, g \in \mathbb{Z}[x]$ be monic polynomials of degree $d \geq 2$. Then the product*

$$\prod_p \frac{f(p)}{g(p)}$$

converges to a nonzero number if and only if the coefficients of x^{d-1} are the same in both polynomials.

Proof If the coefficients of x^{d-1} are equal, then compare the above product with $\zeta(2)$ or $\frac{1}{\zeta(2)}$, otherwise, compare it with $\zeta(1)$ or $\frac{1}{\zeta(1)}$.

Lemma 2. *Let $f, g \in \mathbb{Z}[x]$ be irreducible polynomials for which **Condition 1** holds, and for which their decomposition types are independent of each other. Then **Condition 1** does not hold for their product.*

Proof Let G_f, G_g be the Galois groups of f, g respectively. Let the $\{\mathfrak{C}_f\}, \{\mathfrak{C}_g\}$ be the conjugacy classes for f, g respectively. Then a given decomposition type λ for fg has $n_\lambda = n_{\mathfrak{C}_f} + n_{\mathfrak{C}_g}$ with probability $\frac{|\mathfrak{C}_f||\mathfrak{C}_g|}{|G_f||G_g|}$. The expected number of solutions in $\mathbb{Z}/p\mathbb{Z}$ of fg is

$$\sum_{\mathfrak{C}_f \subset G_f, \mathfrak{C}_g \subset G_g} (n_{\mathfrak{C}_f} + n_{\mathfrak{C}_g}) \left(\frac{|\mathfrak{C}_f||\mathfrak{C}_g|}{|G_f||G_g|} \right) = 2$$

because we can add the expected values for f and g .

Lemma 3.

$$\begin{aligned} E(r; x) &= o(x), \\ E(\mathfrak{C}, G, r; x) &= o(x). \end{aligned}$$

Proof These follow from the Prime Number Theorem and Chebotarëv's Density Theorem respectively.

The following lemma is (5) in [B] and is known as Mertens' Third Theorem.

Lemma 4 (Mertens' Third Theorem).

$$\prod_{p \leq x} \left(1 - \frac{1}{p} \right) \sim \frac{e^{-\gamma}}{\log x}$$

as $x \rightarrow \infty$.

Proof As mentioned in [B], see page 81 of [P].

From Lemmas 1 and 4 we obtain:

Lemma 5. *Let $r_1, r_2 \in \mathbb{Z}$. Then there exists some constant $c_{r_1, r_2} \neq 0$ such that*

$$\prod_{p \leq x} \frac{p - r_1}{p - r_2} \sim c_{r_1, r_2} (\log x)^{r_2 - r_1}$$

as $x \rightarrow \infty$.

Proof By Lemma 4,

$$\prod_{p \leq x} \frac{p}{p-1} \sim e^\gamma \log x$$

as $x \rightarrow \infty$. Now apply Lemma 1 to

$$\prod_p \frac{p - r_1}{p - r_2} \left(\frac{p}{p-1} \right)^{r_1 - r_2}.$$

Merten's Third Theorem was generalized by Uchiyama [U] to primes in congruence classes relatively prime to the modulus 4. Then, it was further generalized by Williams [W] to general arithmetic progressions. This generalization to arithmetic progressions has also been treated in [G],[LZ] and [V]. The following lemma describes this.

Lemma 6 (Williams 1974, Vasil'kovskaja 1977, Grosswald 1987, Languasco, Zaccagnini 2007). *Let $(l, k) = 1$. Then there exists some constant $c_{l,k} \neq 0$ such that*

$$\prod_{\substack{p \leq x \\ p \equiv l \pmod{k}}} \left(1 - \frac{1}{p}\right) \sim c_{l,k} (\log x)^{-1/\varphi(k)}$$

as $x \rightarrow \infty$.

Proof This follows from Theorem 1 of [W]. Or, see any of [G],[LZ], and [V].

As expected, we may obtain Lemma 7 from Lemmas 1 and 6 in the same way that we obtained Lemma 5 from Lemmas 1 and 4.

Lemma 7. *Let $r_1, r_2 \in \mathbb{Z}$. Let $(l, k) = 1$. Then there exists some constant $c_{r_1, r_2, l, k} \neq 0$ such that*

$$\prod_{\substack{p \leq x \\ p \equiv l \pmod{k}}} \left(\frac{p - r_1}{p - r_2}\right) \sim c_{r_1, r_2, l, k} (\log x)^{\frac{r_2 - r_1}{\varphi(k)}}$$

as $x \rightarrow \infty$.

Proof The idea is the same as in Lemma 5.

Now, making use of Theorem 1, we state the following lemma, an analogue of Lemmas 5 and 7.

Lemma 8. *Let $r_1, r_2 \in \mathbb{Z}$. Then there exists some constant $c_{r_1, r_2, \mathfrak{C}, G} \neq 0$ such that*

$$\prod_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C} \subset G}} \left(\frac{p - r_1}{p - r_2}\right) \sim c_{r_1, r_2, \mathfrak{C}, G} (\log x)^{|\mathfrak{C}|(r_2 - r_1)/|G|}$$

as $x \rightarrow \infty$.

Proof Using Theorem 1, the idea is the same as in Lemmas 5 and 7.

From Lemmas 5 and 8 we obtain:

Lemma 9. *Let $r_1, r_2 \in \mathbb{Z}$. Then $Q(\mathfrak{C}, G, r_1, r_2; x)$, defined in (8), converges to a non-zero constant as $x \rightarrow \infty$.*

Condition 2

From (4) and (8), we have

$$C(f) = \prod_{p|\Delta(f)} \left(\frac{p - n_p}{p - 1} \right) \times \lim_{x \rightarrow \infty} \left(\prod_{\mathfrak{C} \subset G} Q(\mathfrak{C}, G, n_{\mathfrak{C}}, 1; x) \right) \times \left(\prod_{p \nmid \Delta(f)} \prod_{\mathfrak{C} \subset G} \left(\frac{p - n_{\mathfrak{C}}}{p - 1} \right)^{|\mathfrak{C}|} \right)^{\frac{1}{|G|}}. \quad (9)$$

By Lemmas 0,1 and 2, the third factor on the right hand side is nonzero or zero according to whether f is irreducible or reducible, respectively, as should be true with $C(f)$ on the left. Therefore, it remains to investigate the second term on the right. Taking its logarithm, we obtain, by (6), (7) and (8),

$$\begin{aligned} & \lim_{x \rightarrow \infty} \log \left(\prod_{\mathfrak{C} \subset G} Q(\mathfrak{C}, G, n_{\mathfrak{C}}, 1; x) \right) \\ &= \lim_{x \rightarrow \infty} \sum_{\mathfrak{C} \subset G} \left(\sum_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C}}} \log(p - n_{\mathfrak{C}}) - \frac{|\mathfrak{C}|}{|G|} \sum_{\substack{p \leq x \\ p \nmid \Delta(f)}} \log(p - n_{\mathfrak{C}}) - \sum_{\substack{p \leq x \\ \sigma_p \in \mathfrak{C}}} \log(p - 1) + \frac{|\mathfrak{C}|}{|G|} \sum_{\substack{p \leq x \\ p \nmid \Delta(f)}} \log(p - 1) \right) \\ &= \lim_{x \rightarrow \infty} \sum_{\mathfrak{C} \subset G} \left(E(\mathfrak{C}, G, n_{\mathfrak{C}}; x) - \frac{|\mathfrak{C}|}{|G|} E(n_{\mathfrak{C}}; x) - E(\mathfrak{C}, G, 1; x) + \frac{|\mathfrak{C}|}{|G|} E(1; x) \right). \end{aligned} \quad (10)$$

Lemma 3 now at least tells us that these terms in the last line are $o(x)$. Sharper bounds would follow from GRH, but even with these, the situation is still not ideal for the use of (9). However, there is a much better way to estimate $Q(\mathfrak{C}, G, n_{\mathfrak{C}}, 1; x)$, and this is contained in Lemma 9. This lemma can be interpreted as saying that the \approx in (5) is sufficient for our purposes if we care only about convergence to a non-zero number or not, and not about the exact value of $C(f)$. Or, in other words, whether $C(f)$ converges to a non-zero number or not, depends only on the third term on the right hand side of (9). From the above, we obtain Theorem 2.

Discussion

In the case where f has abelian Galois group, we need only use Lemma 6, which follows from [G],[LZ],[V] or [W], for Theorem 2. However, in the general case, we need Theorem 1 here for Theorem 2.

Acknowledgements

The author was supported by an AcRF Tier 1 grant at Nanyang Technological University during this work.

References

- [B] S. Baier, A Probabilistic Model for Primes in Random Sets
- [B2] S. Baier, On the Bateman-Horn conjecture, *J. Number Theory* 96 (2002) 432–448
- [BH] P.T. Bateman and R. Horn, A Heuristic Formula concerning the Distribution of Prime Numbers, *Math. Comp.* , 16 (1962), 363–367
- [BZ] S. Baier and L. Zhao, Primes in Quadratic Progressions on Average, *Math. Ann.*, Vol 338, 2007, No. 4, 963–982
- [BZ2] S. Baier and L. Zhao, On Primes in Quadratic Progressions, *Int. J. Number Theory*, Vol 5, 2009, No.6, 1017–1035
- [D] C.S. Dalawat, Splitting Primes, arXiv:1007.4426v3
- [G] E. Grosswald, Some number theoretical products, *Rev. Colombiana Mat.* 21 (1987) 231–242.
- [HL] G.H. Hardy and J.E. Littlewood, Some problems of “Partitio Numerorum”. III On the Expression of a Number as a Sum of Primes. *Acta Math.* 44, 1–70, 1923
- [LS] H.W. Lenstra, Jr. and P. Stevenhagen, Chebotarëv and his Density Theorem, *The Mathematical Intelligencer*, Vol. 18, No. 2, 1996
- [LZ] A. Languasco, A. Zaccagnini, A note on Mertens’ formula for arithmetic progressions, *J. Number Theory* 127 (2007) 37–46
- [P] K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1957
- [S] J-P. Serre, On a Theorem of Jordan, *Bull. Amer. Math. Soc. (N.S.)* 40 (2003), no. 4, 429–440
- [U] S. Uchiyama, On some Products involving Primes, *Proc. Amer. Math. Soc.*, 28 (1971), 629–630
- [V] E.A. Vasil’kovskaja, Mertens’ formula for an arithmetic progression, *Taškent. Gos. Univ. Naučn. Trudy, Voprosy Mat.* 548 (1977) 1417, 139140.
- [V2] F.R. Villegas, *Experimental Number Theory*, Oxford University Press, 2007
- [W] K.S. Williams, Mertens’ Theorem for arithmetic progressions, *J. Number Theory* 6 (1974), 353–359

Div. of Math. Sci., School of Phys. & Math. Sci.,
Nanyang Technological Univ., Singapore 637371
Email: S080074@ntu.edu.sg